Email:support@f-response.com
Website:www.f-response.com
YahooIM:fresponse_s
Phone: 1-800-317-5497

Your Mission: Use F-Response Consultant + Covert to connect to a single target machine.

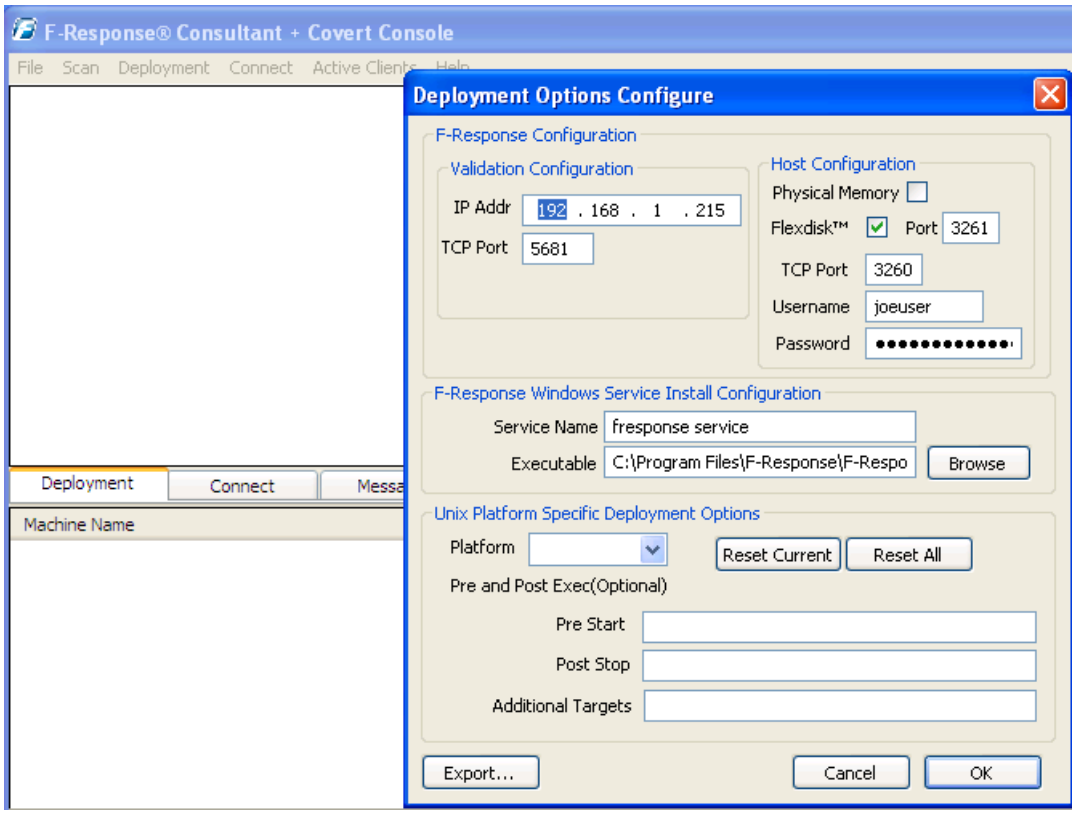
Note: This guide assumes you have installed F-Response Consultant + Covert Edition, your F-Response licensing dongle is plugged into your analyst machine, the F-Response License Manager Monitor is installed and running, and the F-Response Consultant + Console (FC+C) has been started. For more information, please reference the F-Response User Manual.

The F-Response Consultant + Covert Edition provides two GUI tools for using F-Response: the F-Response Consultant Connector (FCC), and the F-Response Consultant + Covert Connector (FC+C). To deploy to a target covertly, we will be using the FC+C which should be started on your analyst machine.

Step 1: Configure the Deployment Options

Before deploy F-Response to the target machine some configuration is required. You will need to configure the Deployment Options Configure, and Credentials Configure windows in the FC+C.

In the FC+C go to File – Configure Options… and the Deployment Options Configure window will open.



Email:support@f-response.com
Website:www.f-response.com
YahooIM:fresponse_s
Phone: 1-800-317-5497

Good news, some of the work here has already been done for you, and typically once you input this information you won't need to change it again. Here is a short overview for each section of the window:

Under the Validation Configuration section, the IP Address of your License Manager (your analyst machine's IP) and default port of 5681 will be populated automatically.

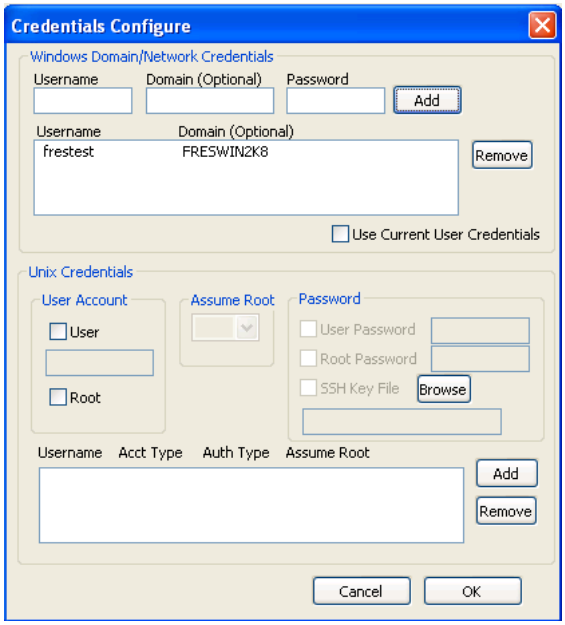
Under the Host Configuration and Windows Service Install Configuration you can enter a username and password for F-Response to use while communicating with your target machine. Go ahead, make it anything you would like. Leave the TCP port default at 3260. If you need access to Flexdisk™, or Physical Memory (for a windows target machine) you also have the option to select it here.

For the F-Response Windows Service Install Configuration, you will need to create and enter a Service Name (again, anything you would like) and select the Windows version of F-Response as the Executable. If you installed F-Response with the standard defaults you can browse to the C:\Program Files\F-Response\F-Response Enterprise Edition directory and choose the f-response-ent.exe file. This will unlock access to the scanning options in later steps.

The "Unix Platform Specific Deployment Options" portion of the window (the lower half) allows you to make temporary exceptions to the *nix firewall for your environment, run scripts, and set additional targets if needed. The defaults provided here should be sufficient such that no action is needed unless you suspect the need to reset to the factory defaults. You can do this by selecting your platform from the list and clicking the Reset Current button. Configuration of the firewall, scripts, and additional targets is beyond the scope of this mission guide.

Step 2: Configure the Target Credentials

Next you need to configure the login credentials to deploy to your target machine. In the FC+C go to File – Configure Credentials… and the Credentials Configure window will open:



Depending on your target machine, you have different options to enter login credentials.

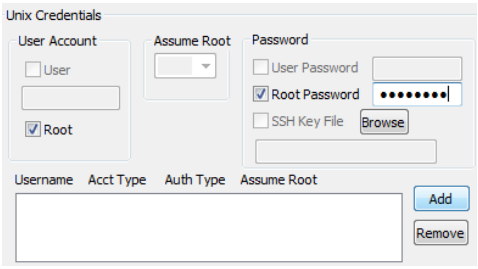
The upper half of the window is used when you need to access a Windows target machine. Simply enter the user name and password for a local account on the target machine, or a domain account by specifying the domain along with the user name and password. Click the Add button and the information is added to the list of credentials F-Response will use to access the Windows target.

The lower half of the window is used when you need access to Unix targets (including Apple). Unix Credentials are covered in detail in Appendix E of the F-Response Manual, but here is a quick overview to accomplish your mission.

Generally there are two types of Unix accounts for our purposes: the all powerful administrator "root" account, and a general user account that can assume root privileges for a time.

Email:support@f-response.com
Website:www.f-response.com
YahooIM:fresponse_s
Phone: 1-800-317-5497

If you have the password for the Root account for the Unix target the process is very simple:

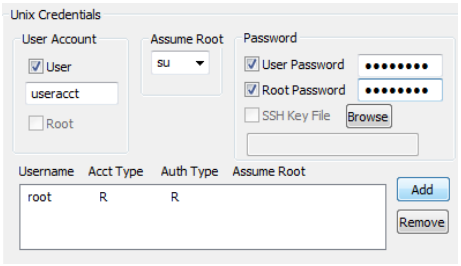


Check the box next to Root under User Account, then check the box for Root Password and enter the password.

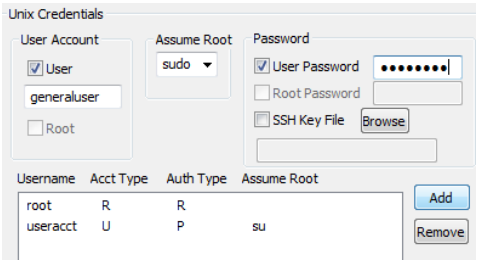
Click the Add button and the information is added to the list of credentials F-Response will use to access the Unix target.

Given the power of the Root account, it is more likely you will be using a general user account that will assume root privileges. The two possibilities for accomplishing this with your user account are su and sudo.

Su is used to assume root level privileges on your Unix target. To configure F-Response to deploy to your Unix target using su:



- Check the box for User in the User Account section and enter your account name.
- Choose su from the Assume Root drop down box.
- Check the box for both User Password and Root Password and enter the passwords.
- Click the Add button to add the account to the list of credentials for F-Response.



Sudo, or "SuperUser Do", is used to execute a command as Root.

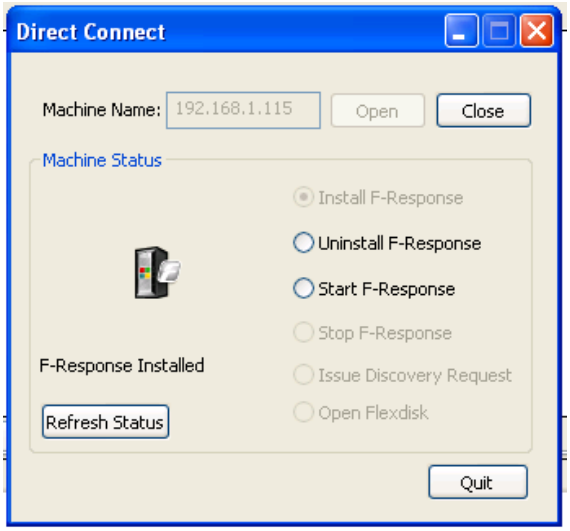
This is your most likely scenario and is a fairly straight forward configuration. Simply check the box for User in the User Account section and enter your account name, choose su from the Assume Root drop down box, then check the User Password box in the Password section and enter your password.

Once you have configured your deployment settings and login credentials you are ready to deploy F-Response covertly to your target machine.

Step 3: Deploy F-Response Covertly to the target machine

Now you ready to deploy F-Response to the target machine. In the FC+C, go to Scan and choose the Direct Connect option. The direct connect window will open:

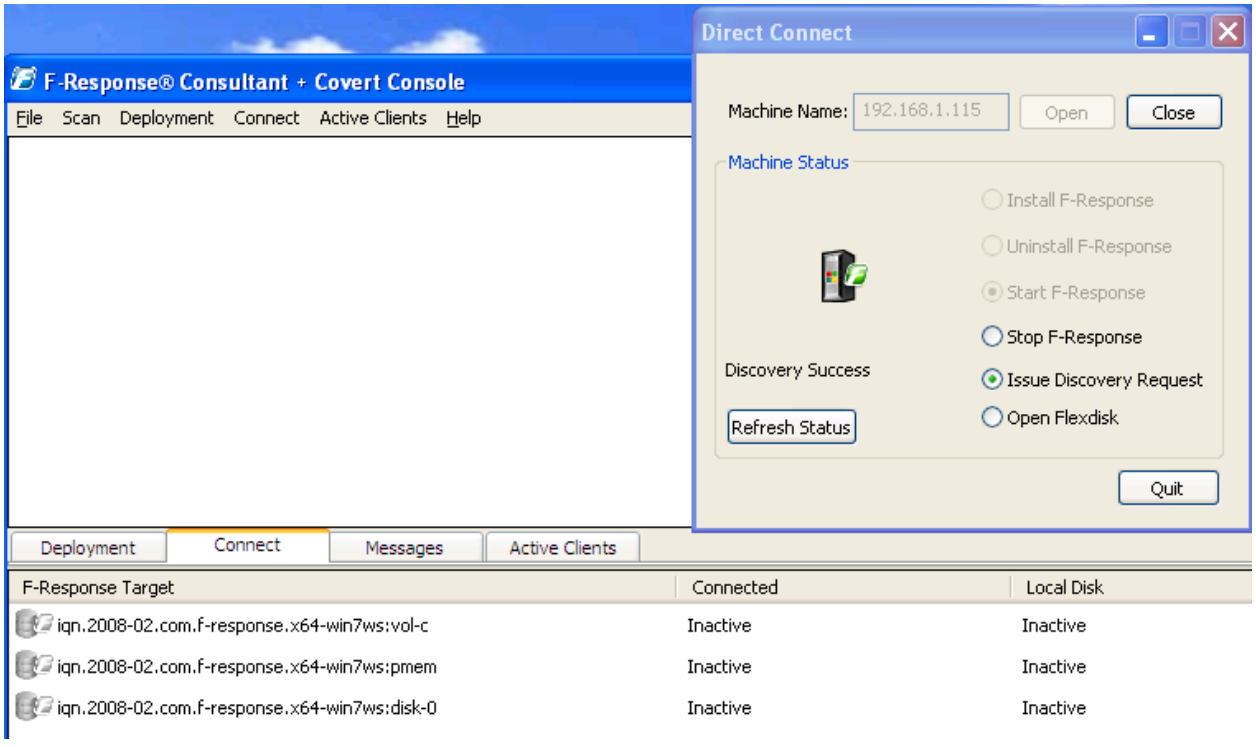
Email:support@f-response.com
Website:www.f-response.com
YahooIM:fresponse_s
Phone: 1-800-317-5497



Here you can enter the target machine's hostname or IP address and click Open. The FC+C will locate your target on the network and present you with the steps to use F-Response on the machine.

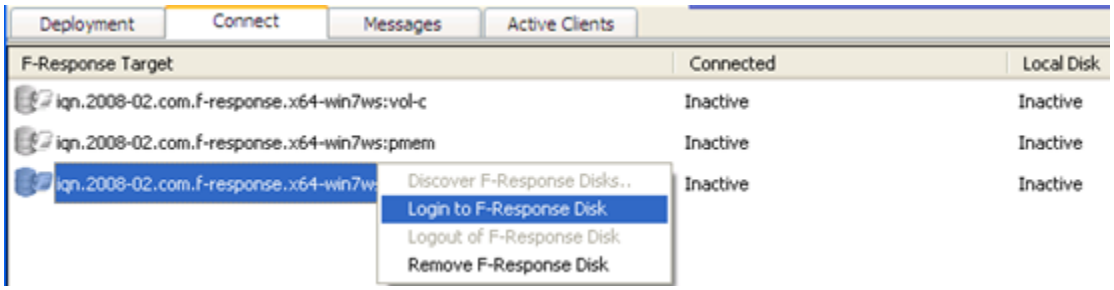
Once you have located the target, click Install F-Response. When the install on the target completes, the icon will display the F-Response badge indicating the installation was successful.

Choose the option to start F-Response on the target machine and the icon will change to green indicating F-Response is now running. Next, choose Issue Discovery Request and then select the Connect tab in the FC+C to get a list of F-Response disks (and memory if selected) available for access.

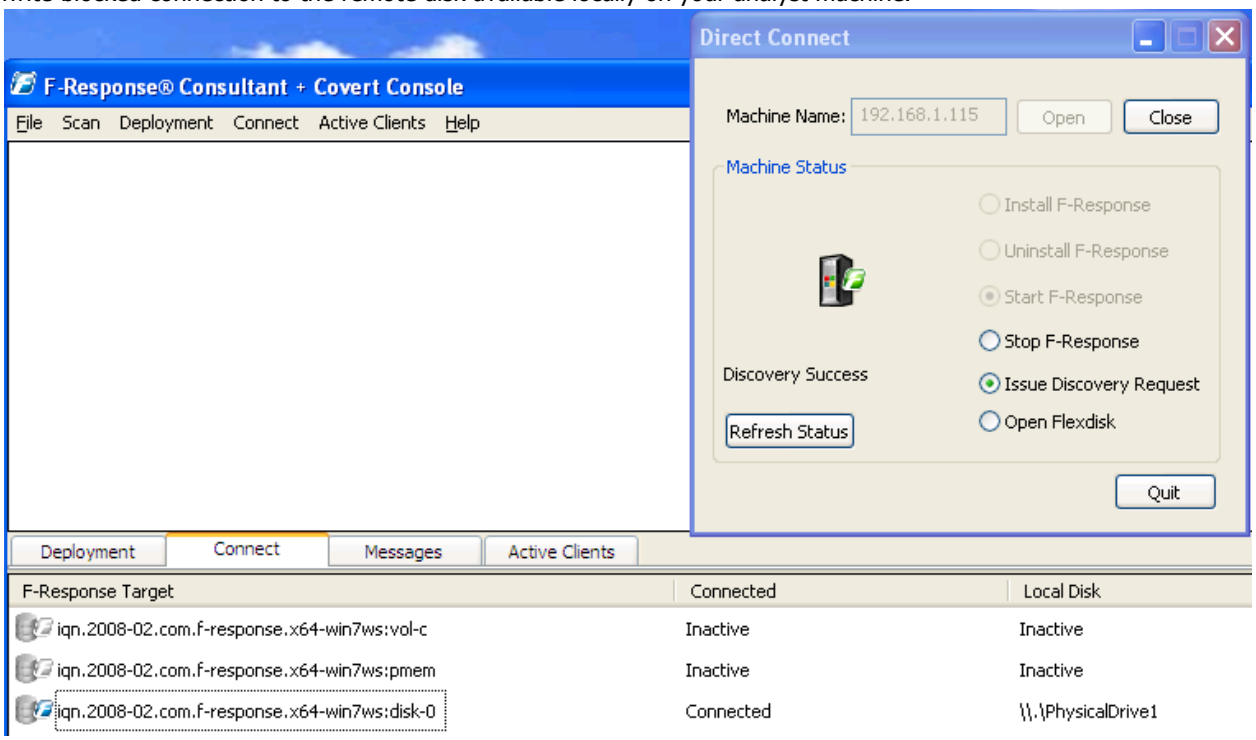


Email:support@f-response.com
Website:www.f-response.com
YahooIM:fresponse_s
Phone: 1-800-317-5497

Right click on the disk you wish to access and login:



The icon will change to blue and the Connected column status will show "Connected" indicating you now have a write-blocked connection to the remote disk available locally on your analyst machine.



Step 4: Fire up the tool of your choice!

F-Response is a vendor neutral product. Once F-Response presents the remote target disk as a write blocked local connection, we step out of your way so that you can select the right tool to get your job done. At this point, you can reach into your toolbox and apply the tool of your choice to the target disk